

Lifting Automorphisms of Quotients by Central Subgroups

Ben Kane, Andrew Shallue

Department of Mathematics
University of Wisconsin-Madison
480 Lincoln Dr
Madison, WI 53706, USA
kane@math.wisc.edu¹, shallue@math.wisc.edu²

ABSTRACT. Given a finitely presented group G , we wish to explore the conditions under which automorphisms of quotients G/N can be lifted to automorphisms of G . We discover that in the case where N is a central subgroup of G , the question of lifting can be reduced to solving a certain matrix equation. We then use the techniques developed to show that $\text{Inn}(G)$ is not characteristic in $\text{Aut}(G)$, where G is a metacyclic group of order p^n , $p \neq 2$.

1. INTRODUCTION

Let F be the free group on n letters, and let G be a quotient of that group. We will be working with a given presentation of G , namely

$$G := \langle x_1, x_2, \dots, x_n \mid r_1(\mathbf{x}), r_2(\mathbf{x}), \dots, r_m(\mathbf{x}) \rangle,$$

where \mathbf{x} represents the n -tuple (x_1, x_2, \dots, x_n) . This vector notation continues throughout the paper. For later ease of exposition, we will think of the relations r_k as noncommutative monomials on n variables (x_1, \dots, x_n) defined by

$$r_k(\mathbf{x}) = \prod_{l=1}^{s_k} x_{j_{k,l}}^{e_{k,l}}$$

with $e_{k,l} \in \{\pm 1\}$.

It is a well known fact that if N is a characteristic subgroup of G , then automorphisms of G induce automorphisms of G/N canonically by acting on the coset representatives. However, much less is known about the conditions under which a lift of an element of $\text{Aut}(G/N)$ exists.

¹now bkane@math.uni-koeln.de

²now ashallue@iwu.edu

Date: April 18, 2013.

2000 *Mathematics Subject Classification.* 20F28.

Key words and phrases. finitely presented group, automorphism group, lift.

Study so far has focused on the case where G is the free group F . Many techniques have been developed to show whether automorphisms of various quotients of F are tame (i.e. for which lifts to F exist). See for instance [1, 2, 5, 6].

We show in the case where N is a central subgroup of an arbitrary group G that automorphisms of G/N are in one-to-one correspondence with solutions to a certain set of matrix equations that depend only on the relations.

ACKNOWLEDGEMENTS

The authors are grateful to N. Boston for giving motivation to the problem and for valuable conversation.

2. HOMOMORPHIC LIFTS

First, assume that G is a finitely presentable group, and N is a cyclic, central subgroup of G , generated by an element z . We will later generalize to the case where N is not cyclic. We wish to study when automorphisms of G/N can be lifted to automorphisms of G . We first give a condition for when such automorphisms lift to homomorphisms of G , so in this section lift means homomorphic lift.

We will also consider G as the image of F under the canonical quotient map $\pi : F \rightarrow F/R$, where R is the normal closure of the set $\{r_1(\mathbf{x}) \dots r_m(\mathbf{x})\}$. However, this will be for convenience only. In practice, working with the relations will suffice, as evidenced by the following lemma, the proof of which is immediate.

Lemma 1. *Let $\theta \in \text{Hom}(F, H)$ be given. Then $\theta(r_k(\mathbf{x})) = 1$ for all k if and only if $\theta(R) = 1$.*

The following definition will help to clarify our direction in this paper:

Definition 1. We say that an n -tuple $\mathbf{g} = (g_1, g_2, \dots, g_n) \in G^n$ extends to a homomorphism if the homomorphism $\theta : F \mapsto G$, defined by $\theta(x_i) = g_i$, factors through R . In this case $\theta \circ \pi^{-1}$ is well defined and defines an element $\psi \in \text{Hom}(G, G)$.

Lemma 2. *An n -tuple $\mathbf{g} \in G^n$ extends to a homomorphism if and only if $r_k(\mathbf{g}) = 1$ for every $k = 1, \dots, m$.*

Proof. Let $\mathbf{g} \in G^n$ be given. Consider θ defined as above. Note that \mathbf{g} extends to a homomorphism if and only if $\theta(R) = 1$. By lemma 1, $\theta(R) = 1$ if and only if $\theta(r_k(\mathbf{x})) = 1$ for all k . So it remains to show that $\theta(r_k(\mathbf{x})) = 1$ if and only if $r_k(\mathbf{g}) = 1$. However, since θ is a homomorphism,

$$\theta(r_k(\mathbf{x})) = r_k(\theta(\mathbf{x})) = r_k(\mathbf{g}).$$

□

The following definition is vital, since homomorphic lifts are the focus of this paper.

Definition 2. A lift of $\varphi \in \text{End}(G/N)$ is $\psi \in \text{End}(G)$ such that

$$\psi(g)N = \varphi(gN) \quad \text{for every } g \in G.$$

Theorem 1. If $\varphi \in \text{End}(G/N)$, then there is a one-to-one correspondence between lifts of φ to $\text{End}(G)$ and n -tuples $\mathbf{g} \in G^n$ such that $g_i N = \varphi(x_i N)$ and $r_k(\mathbf{g}) = 1$ for every $k \in 1, \dots, m$.

Proof. First suppose ψ is a lift of φ . Then by definition $\varphi(x_i N) = \psi(x_i)N$, so we set $g_i := \psi(x_i)$. Also,

$$1 = \psi(1) = \psi(r_k(\mathbf{x})) = r_k(\psi(\mathbf{x})) = r_k(\mathbf{g})$$

since ψ is a homomorphism.

Conversely, suppose we have an n -tuple \mathbf{g} such that $g_i N = \varphi(x_i N)$ and $r_k(\mathbf{g}) = 1$ for every $k = 1 \dots m$. Then by Lemma 2, \mathbf{g} extends to $\psi \in \text{End}(G)$, where $\psi(x_i) = g_i$. Thus

$$\psi(x_i)N = g_i N = \varphi(x_i N)$$

and this is exactly the definition of ψ being a lift of φ . \square

We now give a nice characterization of the lifts of φ . For this we define a certain matrix and a vector.

Define m_{ij} to be the degree of x_j in the commutative image of the word $r_i(\mathbf{x})$. Note that since $r_i(\mathbf{x}) = \prod_{l=1}^{s_i} x_{j_{i,l}}^{e_{i,l}}$,

$$m_{ij} = \sum_{\substack{l \in 1..s_i \\ j_{i,l} = j}} e_{i,l}.$$

We consider the matrix $M := (m_{ij})$. To make the construction of M clear, we give an example.

Example 1. For

$$r_1(\mathbf{x}) = x_1^2 \cdot x_2^{-1} \cdot x_1^{-5} \cdot x_2^{-1}, \quad r_2(\mathbf{x}) = x_1 \cdot x_2^{-3} \cdot x_1^7,$$

we have

$$M = \begin{pmatrix} -3 & -2 \\ 8 & -3 \end{pmatrix}$$

For $\varphi \in \text{Aut}(G/N)$, fix a set of coset representatives $\overline{x_i} \in \varphi(x_i N)$. Since

$$N = \varphi(r_k(\mathbf{x})N) = r_k(\varphi(\mathbf{x}N)) = r_k(\overline{\mathbf{x}})N,$$

it is clear that $r_k(\overline{\mathbf{x}}) \in N$. Since N is generated by z , we can choose w_i such that $r_i(\overline{\mathbf{x}}) = z^{-w_i}$. Note that $\mathbf{w} := (w_1, \dots, w_m)$ is only defined up to the order of N .

Theorem 2. The lifts of φ are in one-to-one correspondence with solutions $\mathbf{v} = (v_1, \dots, v_n)$ to the matrix equation

$$M\mathbf{v} = \mathbf{w} \pmod{\#N}$$

where, if N is infinite, we simply mean the matrix equation on the integers.

Proof. We know from above that lifts are in one-to-one correspondence with $\mathbf{g} \in G^n$ such that $r_k(\mathbf{g}) = 1$ and $g_i N = \varphi(x_i N)$.

However, if $g_i N = \varphi(x_i N) = \overline{x_i} N$, then $g_i \in \overline{x_i} N$. But then $g_i = \overline{x_i} z^{v_i}$ for some i . So $g_i N = \varphi(x_i N)$ if and only if $g_i = \overline{x_i} z^{v_i}$ for some v_i . So lifts are in one-to-one correspondence with $\mathbf{g} \in G^n$ such that $r_k(\mathbf{g}) = 1$ and $g_i = \overline{x_i} z^{v_i}$.

Since z is central,

$$\begin{aligned} r_i(\overline{x_1} z^{v_1}, \dots, \overline{x_n} z^{v_n}) &= r_i(\overline{\mathbf{x}}) r_i(z^{v_1}, z^{v_2}, \dots, z^{v_n}) \\ &= z^{-w_i} z^{\sum_{j=1}^n m_{ij} v_j} \\ &= z^{-w_i + \sum_{j=1}^n m_{ij} v_j} \end{aligned}$$

But this is equal to 1 if and only if $-w_i + \sum_{j=1}^n m_{ij} v_j = 0 \pmod{\#N}$. This corresponds exactly to a solution of the above matrix equation. □

Having shown the result for N cyclic, it is easy to generalize to the case when N is not cyclic.

If N is a central subgroup of G , generated by z_1, \dots, z_t , then we have

$$r_k(\overline{\mathbf{x}}) = z_1^{-w_{1,k}} z_2^{-w_{2,k}} \dots z_t^{-w_{t,k}}$$

Corollary 1. The lifts of φ are in one-to-one correspondence with solutions of the matrix equation

$$\begin{pmatrix} M & & \\ & \ddots & \\ & & M \end{pmatrix} \mathbf{v} = \begin{pmatrix} w_1 \\ \vdots \\ w_t \end{pmatrix} \pmod{\#N},$$

where, if N is infinite, we simply mean the matrix equation on the integers.

Proof. The proof follows from the proof of the previous theorem, noting that each generator of N commutes. □

3. AUTOMORPHIC LIFTS

In this section we investigate when such homomorphic lifts are automorphic. As before, we assume that G is finitely presented and N is a central subgroup of G .

Lemma 3. *If N is abelian, finitely generated, and $\psi \in \text{End}(N)$, then ψ surjective implies ψ injective.*

This lemma follows from the fundamental theorem of abelian groups and the fact that the rank of the image plus the rank of the kernel equals the rank of N .

Lemma 4. *A lift $\psi \in \text{End}(G)$ of $\varphi \in \text{Aut}(G/N)$ is an automorphism if and only if $\psi(N) = N$.*

Proof. Consider $K := \text{Ker}(\psi)$ and $H := \text{Im}(\psi)$.

Since ψ is a lift of φ , we have the identity

$$N = \psi(K)N = \varphi(KN).$$

As φ is injective, it follows that $KN = N$, and hence $K \subseteq N$. So $K = \text{Ker}(\psi|_N)$. Therefore ψ is injective on G if and only if it is injective when restricted to N . Because N is abelian and finitely generated by assumption, it will suffice to show $\psi|_N$ is surjective, even if N is infinite.

Moreover, since $\psi(G)N = \varphi(GN) = G$, it follows that $HN = G$. If $\psi(N) = N$, then $N \subseteq H$, so that $G = HN = H$. Conversely, N is in the image of ψ , and since for $g \in G$, $\psi(g)N = \varphi(gN)$, and $\varphi(gN) = N$ if and only if $g \in N$, we know that the preimage of N is N . So we have ψ surjective if and only if $\psi(N) = N$. □

In the case where $\#N$ is finite and squarefree, the following result will show that the previous work for finding homomorphic lifts will suffice for showing that there is an automorphic lift. The proof relies heavily on finite group theory, for which a good reference is [3].

Theorem 3. *The automorphism φ lifts to $\psi \in \text{End}(G)$ if and only if φ lifts to some $\psi' \in \text{Aut}(G)$.*

Proof. Let $\psi \in \text{End}(G)$ a lift of φ be given. Let $K = \text{Ker}(\psi)$ and $H = \text{Im}(\psi)$. We will show that $G = K \times H$, from which the theorem follows directly, since $\psi|_H$ is an isomorphism and $(\text{Id}, \psi|_H)$ will be a lift as desired, where Id stands for the identity on K .

From the proof of Lemma 4, $K \subseteq N$. Since $\#N$ is squarefree and N is abelian, it splits completely. In particular, by the first isomorphism theorem, $N = K \times H_N$, where $H_N = \text{Im}(\psi|_N)$. We know from the above proof that $HN = G$. Then

$$G = H(K \times H_N) = (HK)(HH_N) = HKH = HK.$$

Let $h \in H \cap K$ be given. Notice first that $\text{Im}(\psi) \cap N = \text{Im}(\psi|_N)$ since the preimage of N is contained in N . Since $h \in K \subseteq N$, we have $h \in H_N$. But $H_N \cap K = 1$, so $h = 1$. Hence $G = H \rtimes K$. Therefore, since K is central, $G = H \times K$. □

We are now going to construct a set of matrix equations whose solutions correspond to automorphic lifts of φ . Let us first assume N is cyclic and generated by z . The key idea is that matching exponents of z reduces to solving linear equations. We first fix a noncommutative monomial

$$f(\mathbf{x}) := \prod_{l=1}^s x_{j_l}^{e_l}$$

such that $f(\mathbf{x}) = z$. Define

$$M_{m+1,j} := \sum_{\substack{l \in 1..s \\ j_l = j}} e_l,$$

which is the exponent of x_j in the commutative image of $f(\mathbf{x})$. Since $\varphi(N) = N$, we can choose w_{m+1} such that $z^{-w_{m+1}} = f(\overline{\mathbf{x}})$, where $\overline{\mathbf{x}}_i$ is as above.

For an automorphism, the image of z must be a generator of N . We will define a matrix equation for each of the possible generators of N . For N infinite, define $w_{m+1}^{(1)} := w_{m+1} + 1$ and $w_{m+1}^{(2)} := w_{m+1} - 1$ and set

$$M' := \begin{pmatrix} M \\ M_{m+1} \end{pmatrix}.$$

For N finite, with p the smallest prime dividing $\#N$, define $w_{m+1}^{(k)} := w_{m+1} + k \frac{\#N}{p}$ for $k = 1, \dots, p-1$ and set

$$M' := \begin{pmatrix} M \\ \frac{\#N}{p} M_{m+1} \end{pmatrix}.$$

In either case, set $\mathbf{w}^{(k)} := \begin{pmatrix} \mathbf{w} \\ w_{m+1}^{(k)} \end{pmatrix}$ for every k .

Theorem 4. *Automorphic lifts of $\varphi \in \text{Aut}(G/N)$ are in one-to-one correspondence with solutions $\mathbf{v} = (v_1, \dots, v_n)$ to the matrix equations*

$$M' \mathbf{v} = \mathbf{w}^{(k)} \pmod{\#N}$$

for $k = 1, 2$ if N is infinite, and $k = 1, \dots, p-1$ for N finite and p the smallest prime dividing $\#N$.

Proof. For a solution \mathbf{v} to the equation $M \mathbf{v} = \mathbf{w}$, we have a lift $\psi \in \text{End}(G)$ by Theorem 2. By Lemma 4, $\psi \in \text{Aut}(G)$ if and only if $\psi(z)$ generates N . But then

$$\begin{aligned} \psi(z) &= f(\psi(\mathbf{x})) = f(\overline{x}_1 z^{v_1}, \dots, \overline{x}_n z^{v_n}) \\ &= f(\overline{\mathbf{x}}) f(z^{\mathbf{v}}) = z^{-w_{m+1} + \sum_{j=1}^n m_{m+1,j} v_j} \end{aligned}$$

If N is infinite we need $\psi(z) = z^{\pm 1}$ to generate N . This is equivalent to $-w_{m+1} + \sum_{j=1}^n m_{m+1,j} v_j = \pm 1$. These are exactly the matrix equations listed above.

If N is finite, then we need $o(\psi(z)) = \#N$, so we simply need $\psi(z)^{\frac{\#N}{p}} \neq 1$. But this is equivalent to

$$-\frac{\#N}{p} w_{m+1} + \frac{\#N}{p} \sum_{j=1}^n m_{m+1,j} v_j \neq 0 \pmod{\#N}.$$

But, if this sum is not 0, it must be $k \frac{\#N}{p}$ for some $k = 1, \dots, p-1$. These correspond to the above vectors. \square

Similarly to above, we can generalize this to the case when N is not cyclic.

If N is generated by z_1, \dots, z_t , then, following the above process, we can choose a presentation of each element z_i and add another row to M with this presentation, generating a matrix M'' . Next, we choose for each z_i an element of z'_i of N which we would like to map z_i to, such that the z'_i also generate N . Note that z'_i must have the same order as z_i , since we have a homomorphism.

We write for each k from 1 to the number of possible generator sets of N

$$z'_i = \prod_{j=1}^t z_j^{w_{i,m+j}^{(k)}}.$$

Corollary 2. Automorphic lifts of $\varphi \in \text{Aut}(G/N)$ are in one-to-one correspondence with solutions to the matrix equations

$$\begin{pmatrix} M'' & & \\ & \ddots & \\ & & M'' \end{pmatrix} \mathbf{v} = \begin{pmatrix} w_1^{(k)} \\ \vdots \\ w_t^{(k)} \end{pmatrix} \pmod{\#N},$$

Remark. Note that if we have 2 elements of infinite order as generators of N , then there are infinitely many choices for our $\mathbf{w}^{(k)}$, but otherwise we have a finite number of choices as above.

4. AN APPLICATION OF THE ABOVE TECHNIQUES

In this section, we give an application of the techniques developed above. Given a metacyclic group of order p^n (p an odd prime) represented by

$$G := \langle x, y \mid x^{p^{n-1}}, y^p, x^y = x^{1+p^{n-2}} \rangle,$$

we will show that $\text{Inn}(G)$ is not characteristic in $\text{Aut}(G)$.

To do this, we need information about the structure of $A := \text{Aut}(G)$. Schulte in [4] found the presentation for A

$$A = \left\langle x_1, x_2, x_3 \left| \begin{array}{l} x_1^p, x_2^p, x_3^{(p-1)p^{n-2}}, x_1^{-a} \cdot x_3^{-1} \cdot x_1 \cdot x_3 \cdot x_3^{j(p-1)p^{n-3}}, \\ x_2^{-a^{-1}} \cdot x_3^{-1} \cdot x_2 \cdot x_3 \cdot x_3^{k(p-1)p^{n-3}}, x_1^{-1} \cdot x_2^{-1} \cdot x_1 \cdot x_2 \cdot x_3^{-(p-1)p^{n-3}} \end{array} \right. \right\rangle,$$

where a is a generator for the multiplicative group $(\mathbb{Z}/p^{n-2}\mathbb{Z})^\times$, a^{-1} is the multiplicative inverse \pmod{p} , and j and k are integers which can be determined explicitly.

We shall henceforth refer to the center of A as $Z := Z(A)$. By the commutator relations above $\langle x_3^{p-1} \rangle \subseteq Z$. Note that $A/\langle x_3^{p-1} \rangle$ equals $(C_p \times C_p) \rtimes C_{p-1}$. Since that group has trivial center, by the correspondence theorem, $\langle x_3^{p-1} \rangle = Z$. For ease of exposition, we will denote x_3^{p-1} by z .

Another important fact is that $I := \text{Inn}(G) = \langle x_1, x_3^{(p-1)p^{n-3}} \rangle$. This follows from [4] by showing that conjugation by x and y correspond to the elements x_1 and $x_3^{(p-1)p^{n-3}}$, respectively.

From Section 1, we have a technique for determining when homomorphisms can be lifted from quotient groups. Since Z is large, cyclic, central, and characteristic in A , A/Z is a natural candidate for this process.

We will show that all elements of $\text{Aut}(A/Z)$ lift to $\text{Aut}(A)$, and then show that some $\varphi \in \text{Aut}(A/Z)$ does not fix IZ/Z . We then conclude that some $\psi \in \text{Aut}(A)$ does not fix IZ and so IZ is not characteristic in A . Since Z is characteristic, it follows that I is not characteristic.

Theorem 5. *The canonical mapping $\pi : \text{Aut}(A) \mapsto \text{Aut}(A/Z)$ is surjective.*

Proof. Let $\varphi \in \text{Aut}(A/Z)$ be given and set $K := \langle x_1, x_2 \rangle$. Studying K in some detail will simplify the ensuing calculations.

Since KZ is the unique Sylow p -subgroup of A/Z , it is characteristic, and hence $\varphi(KZ) = KZ$. Therefore, without loss of generality, we can choose representatives $(\overline{x_1}, \overline{x_2}, \overline{x_3})$ such that $\varphi(x_i Z) = \overline{x_i} Z$ and $\overline{x_1}, \overline{x_2} \in K$.

Since A/K is cyclic and hence abelian, it follows that $A' \subseteq K$. Notice that $K \cap Z = \langle [x_1, x_2] \rangle = \langle z^{p^{n-3}} \rangle$ and $K^p = 1$. Also, the exponent of A is $(p-1)p^{n-2}$, so $A^{(p-1)p^{n-3}}$ contains only elements of order p , and hence is contained in K , since every element of order p is in K .

Since Z is cyclic and central, Theorem 2 tells us that homomorphisms of A that are lifts of φ are in one-to-one correspondence with solutions to

$$\begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & (p-1)p^{n-2} \\ 1-a & 0 & j(p-1)p^{n-3} \\ 0 & 1-a^{-1} & k(p-1)p^{n-3} \\ 0 & 0 & -(p-1)p^{n-3} \end{pmatrix} \begin{pmatrix} v \\ v \\ v \end{pmatrix} = \begin{pmatrix} w \\ w \\ w \end{pmatrix} \pmod{\#Z}.$$

So φ lifts to a homomorphism if and only if this matrix is not degenerate. We shall show that this matrix has p^{n-3} solutions.

Instead of calculating \mathbf{w} , we only need to show that $w_1, w_2, w_3 = 0$, and $p^{n-3} \mid w_4, w_5, w_6$. Notice that the latter statement is equivalent to $z^{w_i} \in K$.

For $i = 1, 2$, we note that $K^p = 1$ and for $i = 3$, we have $r_3(\overline{\mathbf{x}}) = 1$ because the exponent of A is $(p-1)p^{n-2}$, so any choice for $\overline{x_3}$ will give $w_3 = 0$.

For $i = 4, 5, 6$, notice that since $\overline{x_1}, \overline{x_2} \in K$,

$$r_i(\overline{\mathbf{x}}) \in KA'A^{(p-1)p^{n-3}}.$$

From our comments above, we know that $A', A^{(p-1)p^{n-3}} \subseteq K$. Hence $r_i(\overline{\mathbf{x}}) \in K$, and we have $p^{n-3} \mid w_i$.

Since the matrix is taken mod $\#Z = p^{n-2}$, the third row of the matrix is all zeroes and $w_3 = 0$, so we can remove this redundancy. Rows 1 and 2 correspond to $pv_1 = 0$ and $pv_2 = 0$, respectively. This is equivalent to $p^{n-3} \mid v_1, v_2$.

Therefore, if \mathbf{v} is a solution, it must be the case that $p^{n-3} \mid v_1, v_2$. Hence, we can remove the first three rows and write the matrix in the form:

$$p^{n-3} \begin{pmatrix} (1-a) & 0 & j(p-1) \\ 0 & (1-a^{-1}) & k(p-1) \\ 0 & 0 & -(p-1) \end{pmatrix} (\mathbf{v}) = p^{n-3} \left(\frac{\mathbf{w}}{p^{n-3}} \right) \pmod{\#Z}$$

With $v_1, v_2 \in \mathbb{Z}/p\mathbb{Z}$, and $v_3 \in \mathbb{Z}/p^{n-2}\mathbb{Z}$.

Solutions to this matrix will correspond to solutions of

$$\begin{pmatrix} 1-a & 0 & -j \\ 0 & 1-a^{-1} & -k \\ 0 & 0 & 1 \end{pmatrix} (\mathbf{v}) = \left(\frac{\mathbf{w}}{p^{n-3}} \right) \pmod{p}$$

The determinant of this matrix is $D := (1-a)(1-a^{-1})$, but a is a generator for the multiplicative group $(\mathbb{Z}/(p^{n-1}\mathbb{Z}))^\times$, so $a \not\equiv 1 \pmod{p}$ and $a^{-1} \not\equiv 1 \pmod{p}$. Thus, D is invertible, so the matrix is solvable. Moreover, since $v_3 \in \mathbb{Z}/p^{n-2}\mathbb{Z}$, and this solution only fixes $v_3 \pmod{p}$, we have p^{n-3} choices for v_3 , and hence φ lifts to p^{n-3} homomorphisms of A .

We would now like to show that each of these homomorphisms is moreover an automorphism. By Lemma 4, we know that ψ is an automorphic lift exactly when $\psi(z)^{p^{n-3}} = [\psi(x_1), \psi(x_2)] \neq 1$.

Lemma 5. *We have the equality*

$$Z(K) = Z \cap K.$$

Proof. Let $h = x_1^a x_2^b \left(z^{p^{n-3}} \right)^c \in Z(K)$ be given. Then, since $[x_1, x_2] = z^{p^{n-3}}$,

$$hx_1 = x_1 h \left(z^{p^{n-3}} \right)^{-b} \text{ and } hx_2 = x_2 h \left(z^{p^{n-3}} \right)^a.$$

Thus, $b = 0 = a$. □

We see that for $h \in K \setminus Z(K)$, $C_K(h) = \langle h \rangle Z(K)$, since

$$p^3 = \#K > \#C_K(h) \geq p^2.$$

But $\psi(x_1) \notin \langle \psi(x_2) \rangle Z(K)$, as $\varphi(x_1 Z) \notin \langle \varphi(x_2 Z) \rangle$. Therefore, since $\psi(x_1)$ and $\psi(x_2)$ do not commute, $[\psi(x_1), \psi(x_2)] \neq 1$. So the canonical mapping is surjective. □

We will now proceed to show that IZ/Z is not characteristic in A/Z . Note that

$$A/Z = (IZ \times HZ) \rtimes \langle x_3 \rangle Z \cong (C_p \times C_p) \rtimes C_{p-1},$$

with the action of x_3 on IZ being $x \mapsto x^a$ and the action of x_3 on HZ being $x \mapsto x^{a^{-1}}$.

We would like to show that $(\overline{\mathbf{x}}) = \left(x_2^{a^{-1}}, x_1^a, x_3^{-1} \right)$ extends to a homomorphism. The presentation for A/Z is the same as the presentation for A , adding the relation that

$z = x_3^{p-1} = 1$. It is straightforward to calculate that $r_k(\overline{\mathbf{x}}) = 1$ for every k . Moreover, $\langle x_2^{a^{-1}}, x_1^a, x_3^{-1} \rangle = A/Z$, so this homomorphism is an automorphism. This automorphism is the desired element of $\text{Aut}(A/Z)$.

REFERENCES

- [1] S. Andreadakis, On the Automorphisms of Free Groups and Free Nilpotent Groups., Proc. London Math. Soc. (3) 15 (1965) 239-268.
- [2] S. Bachmuth, Automorphisms of Free Metabelian Groups, Trans. Amer. Math. Soc. 118 (1965) 93-104.
- [3] S. Lang, Algebra, Addison-Wesley, Reading, 1993.
- [4] M. Schulte, Automorphisms of Metacyclic p -groups With Cyclic Maximal Subgroups, Rose-Hulman Undergraduate Mathematics Journal 2 (2001) (available at <http://www.rose-hulman.edu/mathjournal/2001/vol2-n2/paper4/v2n2-4pd.pdf>).
- [5] V. Shpilrain, Non-Commutative determinants and automorphisms of groups, Comm. Algebra 25 (1997) 559-574.
- [6] E. Turner, D. Voce, Tame Automorphisms of Finitely Generated Abelian Groups, Proc. Edinburgh Math. Soc. 41 (1998) 277-287.